DEPARTMENT OF DEFENSE INFORMATION SECURITY PROGRAM REGULATION

CHAPTER I

GENERAL PROVISIONS

Section 1

REFERENCES

1-1oo References

(f) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
(g) Executive Order (E.O.) 12356, "National Security Information," April 2, 1982
(h) Information Security Oversight Office (1S00) Directive No. 1, "National Security Information,"' June 23, 1982
(i) DoD Directive 5220.22, "Department of Defense Industrial Security Program," December 8, 1980
(j) DoD 5220.22-R, "Industrial Security Regulation," December 1985 (or current edition)
(k) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," December 1985 (or current edition)
(1) Public Law 83-703, "Atomic Energy Act of August 30, 1954," as amended
(m) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972
(n) DoD 5200.28-M, "ADP Security Manual: Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems," January 1973
(o) E.O. 12333, "United States Intelligence Activities," December 4, 1981
(P) DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980
(q) Title 35, United States Code, Sections 181-188, "The Patent Secrecy Act of 1952"
(r) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
(s) DoD 5200.1-H, "Writing Security Classification Guidance Handbook," October 1980
(t) DoD 5200.1-1, "DoD Index of Security Classification Guides" 1/
(u) DoD Directive 5535.2, "Delegations of Authority to Secretaries of the Military Departments - Inventions and Patents," October 16, 1980
(v) DoD Directive 5200.30, "Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records," September 9, 1981
(w) Title 31, United States Code, Section 483a (Title 5, Independent Offices Appropriation Act)
(x) DoD Instruction 7230.7, "User Charges," June 12, 1979
(Y) DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS)," October 17, 1978
(z) DoD Instruction 5230.22, "Control of Dissemination of Intelligence Information," April 1, 1982

---

l_/ Published on an annual basis.

(aa) National COMSEC Instruction 4005, "Safeguarding and Control of COMSEC Material," October 12, 1979

(bb) National Communications Security Committee (NCSC) Policy Directive 6, January 16, 1981

(cc) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," October 6, 1981

(old) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978

(ee) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982

(ff) Joint Army-Navy-Air Force Publications (JANAP) #119 and #299

(gg) DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program," February 26, 1986

(hh) E.O. 12065, "National Security Information," June 28, 1978

(ii) DoD Directive 5210.56, "Use of Force by Personnel Engaged in Law Enforcement and Security Duties," May 10, 1969

(jj) DoD Directive 5030.47, "National Supply System," May 27, 1971

(kk) Memorandum by the Secretary, Joint Chiefs of Staff (SM) 701-76, Volume II, "Peacetime Reconnaissance and Certain Sensitive Operations," July 23, 1976

(11) DoD Directive 3224.3, "Physical Security Equipment: Assignment of Responsibility for Research, Engineering, Procurement, Installation, and Maintenance," December 1, 1976

(mm) National COMSEC Instruction 4009, "Protected Distribution Systems," December 30, 1981

(nn) DoD Directive 5200.12, "Policy on the Conduct of Meetings Involving Access to Classified Information," September 24, 1984

(00) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," July 28, 1983

(pp) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," October 18, 1982

(qq) DoD 5200.2-R, "DoD Personnel Security Program," December 1979

(rr) DoD Directive 5400.4, "Provision of Information to Congress," January 30, 1978

(ss) DoD Directive 7650.1, "General Accounting Office Comprehensive Audits," July 9, 1958

(tt) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984

(uu) Title 50, United States Code, Section 403, "National Security Act"

(w) DoD Directive 4540.1, "Use of Airspace for United States Military Aircraft and Firings Over the High Seas," January 13, 1981

(ww) DoD Directive 5210.41, "Security Criteria and Standards for Protecting Nuclear Weapons," September 12, 1978

(xx) DoD Instruction 1000.13, "Identification Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Personnel," July 16, 1979

(yy) Public Law 76-443, "Espionage Act," March 28, 1940

(Zz) Title 10, United States Code, Section 801 et seq, "Uniform Code of Military Justice"

(aaa) Allied Communication Publication (ACP) #110

(bbb) DoD Directive 5230.24, “Distribution Statements on Technical Documents,” November 20, 1984

(ccc) DoD 5200.1-PH-1, “Classified Information Nondisclosure Agreement (SF 189),” July 1985

(ddd) DoD 5200.1-PH, “A Guide to Marking Classified Documents,” November 1982

(eee) DoD Directive C-5230.23, “Intelligence Disclosure Policy,” November 18, 1983

(fff) DoD Instruction 5230.20, “Control of Foreign Representatives,” June 25, 1984

(ggg) DoD TS-5105.21-M-2, "SCI Security Manual - Communications Intelligence Policy,” July 1985

(hhh) DoD C-5105.21-M-1, “SCI Security Manual - Administrative Security,” January 1985

(iii) DoD TS-5105.21-M-3, "SCI Security Manual - TK Policy,” November 1985

(jjj) National COMSEC Instruction 4003, “Classification Guidelines for COMSEC Information,” December 1, 1978

(kkk) National COMSEC Instruction 4006, “Reporting COMSEC Insecurities,” October 20, 1983

(lll) National Telecommunications and Information Systems Security Instruction 4001, “Controlled Cryptographic Items,” March 25, 1985

(mMm) National COMSEC Instruction 4008, “Safeguarding COMSEC Facilities,” March 4, 1983

(nnn) DoD Directive 5405.2, “Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses,” July 23, 1985

(000) DOD DIRECTIVE 5122.5, “ASSISTANT SECRETARY OF DEFENSE (PUBLIC AFFAIRS),” JUNE 15, 1982

(ppp) DOD DIRECTIVE 5230.9, “CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE,” APRIL 2, 1982

(qqq) DIA MANUAL 50-3, “PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES,” MAY 2, 1980

(rrr) ADMINISTRATIVE INSTRUCTION NO. 15, “OSD RECORDS MANAGEMENT PROGRAM,” APRIL 28, 1981

(sss) ADMINISTRATIVE INSTRUCTION NO. 23, “PERSONNEL SECURITY PROGRAM AND CIVILIAN PERSONNEL SUITABILITY PROGRAM,” FEBRUARY 25, 1986

(ttt) ARMY REGULATION 27-10, “MILITARY JUSTICE,” June 1, 1984

(uuu) AIR FORCE REGULATION 35-32, “UNFAVORABLE INFORMATION FILES, CONTROL ROSTERS, ADMINISTRATIVE REPRIMANDS, AND ADMONITIONS,” February 12, 1982

(VW) THE NAVY AND MARINE CORPS, “JUDGE ADVOCATE MANUAL 5800.78”, July 17, 1984

(www) DIA MANUAL 50-1, “SENSITIVE COMPARTMENTED INFORMATION (SCI) SECURITY MANAGEMENT , “ SEPTEMBER 10, 1984

(xxx) “THE UNIFORM CODE OF MILITARY JUSTICE”

(yyy) DoD 5400. 7-R, “DOD FREEDOM OF INFORMATION ACT PROGRAM, “ DECEMBER 1980

(zzz) TITLE 5, UNITED STATES CODE, “THE FREEDOM OF INFORMATION ACT, “ SECTION 552

(aaaa) DOD DIRECTIVE 5230.24, “DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS, “ NOVEMBER 20, 1984

(bbbb) DoD Directive 5240.5, “DoD Technical Surveillance Countermeasures (TSCM) Survey Program, ” May 24, 1984

Section 2

PURPOSE AND APPLICABILITY

1“200 Purpose

Information of the Department of Defense relating to national security shall be protected against unauthorized disclosure as long as required by national security considerations. This Regulation establishes a system for classification, downgrading and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations.

1-201 Applicability

This Regulation governs the DoD Information ‘Security Program and takes precedence over all DoD Component regulations that implement that Program. Under DoD Directive 5200.1, E.O. 12356, and ISOO Directive No. 1 (references (f), (g), and (h)), it establishes, for the Department of Defense, uniform policies, standards, criteria, and procedures for the security classification, downgrading, declassification, and safeguarding of information that is owned by, produced for or by, or under the control of the Department of Defense or its Components.

1-202 Nongovernment Operations

Except as otherwise provided herein, the provisions of this Regulation that are relevant to operations of nongovernment personnel entrusted with classified information shall be made applicable thereto by contracts or other legally binding instruments. (See DoD Directive 5220.22, DoD 5220.22-R, and DoD 5220.22-M, references (i), (j) and (k)).

1-203 Combat Operations

The provisions of this Regulation relating to accountability, dissemination, transmission, or safeguarding of classified information may be modified by military commanders but only to the extent necessary to meet local conditions in connection with combat or combat-related operations. Classified information should be introduced into forward combat areas or zones or areas of potential hostile activity only when essential to accomplish the military mission.

1-204 Atomic Energy Material

Nothing in this Regulation supersedes any requirement related to “Restricted Data” in the Atomic Energy Act of August 30, 1954, as amended (reference (l)), or the regulations of the Department of Energy under that Act. “Restricted Data” and material designated as “Formerly Restricted Data,” shall be handled, protected , classified, downgraded, and declassified to conform with reference (1) and the regulations issued pursuant thereto.

1-205 Sensitive Compartmented and Communications Security Information

a. Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information shall be handled and controlled in accordance with applicable national directives and DoD Directives and Instructions. Other classified

information, while in established SCI or COMSEC areas , may be handled in the same reamer as SCI or COMSEC information. Classification principles and procedures, markings, downgrading, and declassification actions prescribed in this Regulation apply to SCI and COMSEC information. (See also paragraph 13-200 C.).

b. Pursuant to DoD Directive 5200.1 (reference (f)), the Director, National Security Agency/Chief, Central Security Service may prescribe special rules and procedures for the handling, reporting of loss, storage, and access to classified communications security devices, equipments, and materials in mobile, hand-held or transportable systems, or that are used in conjunction with commercial telephone systems, or in similar circumstances where operational demands preclude the application of standard safeguards. These special rules may include procedures for safeguarding such devices and materials, and penalties for the negligent loss of government property.

1-206 Automatic Data Processing Systems

This Regulation applies to protection of classified information processed, stored or used in, or communicated, displayed or disseminated by an automatic data processing (ADP) system. Additional security policy, responsibilities, and requirements applicable specifically to ADP systems are contained in DoD Directive 5200.28 and DoD 5200.28-M, references (m) and (n).

1-207 SUGGESTIONS FOR CHANGES

USERS OF THIS INSTRUCTION ARE ENCOURAGED TO SUBMIT SUGGESTIONS FOR IMPROVING OF THIS INSTRUCTION TO THE PHYSICAL SECURITY DIVISION (PSD), WHS. COMMENTS SHOULD INDICATE THE SPECIFIC PAGE(S), PARAGRAPH(S) AND LINE(S) OF THE TEXT TO BE CHANGED. RATIONALE SHALL ACCOMPANY EACH RECOMMENDED CHANGE.

Section 3

DEFINITIONS

1-300 Access

The ability and opportunity to obtain knowledge of classified information.

1-301 Applicable Associated Markings

The markings, other than classification markings, and warning notices listed or referred to in subsection 4-103.

1-302 Carve-Out

A classified contract issued in connection with an approved Special Access Program in which the Defense Investigative Service has been relieved of inspection responsibility in whole or in part under the Defense Industrial Security Program.

1-303 Classification Authority

The authority vested in an official of the Department of Defense to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

1-304 Classification Guide

A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively. For purposes of this Regulation, this term does not include DD Form 254, "Contract Security Classification Specification."

1-305 Classified Information

Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under E.O. 12356 (reference (g)) or prior orders and this Regulation to require protection against unauthorized disclosure; and (c) so designated.

1-306 Classifier

An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

1-307 Communications Security (COMSEC)

The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications . COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COSMEC material and information.

1-308 Compromise

The disclosure of classified information to persons not authorized access thereto.

1-309 Confidential Source

Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

1-310 Continental United States (CONUS)

United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

1-311 Controlled Cryptographic Item (CCI)

A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled. (Note: Equipments and components so designated bear the designator "Controlled Cryptographic Item" or "CCI.")

1-312 Critical Nuclear Weapon Design Information

That Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test, or replace.

1-313 Custodian

An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

1-314 Declassification

The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation.

1-315 Declassification Event

An event that eliminates the need for continued classification of information.

1-316 Derivative Classification

A determination that information is in substance the same as information currently classified, and the application of the classification ❑ arkings.

1-317 Document

Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, engravings, sketches, working notes and papers, or reproductions by any means or process, and sound, voice, magnetic or electronic recordings in any form.

1-318 DoD Component

The Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

1-319 Downgrade

A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such lower degree of protection.

1-320 Foreign Government Information

Information that is (a) provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or (b) produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

1-321 Formerly Restricted Data

Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same reamer as Restricted Data.

1-322 Information

Knowledge that can be communicated by any means.

1-323 Information Security

The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

1-324 Intelligence Activity

An activity that an agency within the Intelligence Community is authorized to conduct under E.O. 12333 (reference (o)).

1-325 Material

Any product or substance on, or in which, information is embodied.

1-326 National Security

The national defense and foreign relations of the United States.

1-327 Need-to-know

A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of the classified information in order to accomplish lawful and authorized Government purposes.

1-328 Original Classification

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

1-329 Regrade

A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

1-330 Restricted Data

All data concerning (a) design, manufacture or utilization of atomic weapons; (b) the production of special nuclear material; or (c) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under Section 142 of reference (l). (See also Section lly, Atomic Energy Act of 1954, as amended, and "Formerly Restricted Data," subsection 1-318.)

1-331 Security Clearance

A determination that a person is eligible under the standards of DoD 5200.2-R (reference (qq)) for access to classified information.

1-332 Sensitive Compartmented Information

Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

1-333 Special Access Program

Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine need-to-know; or special lists of persons determined to have a need-to-know.

1-334 Special Activity

An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so

that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

1-335 Unauthorized Disclosure

A communication or physical transfer of classified information to an unauthorized recipient.

1-336 United States and Its Territories, Possessions, Administrative, and Commonwealth Areas

The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, and the Virgin Islands; the Trust Territory of the Pacific Islands; and the Possessions, Midway and Wake Islands.

1-337 Upgrade .

A determination that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree.

1-338 FOR OFFICIAL USE ONLY (FOUO)

INFORMATION THAT HAS NOT BEEN GIVEN A SECURITY CLASSIFICATION UNDER THE CRITERIA OF AN EXECUTIVE ORDER, BUT THAT MAY BE WITHHELD FROM THE PUBLIC FOR ONE OR MORE OF THE REASONS CITED IN FREEDOM OF INFORMATION ACT EXEMPTIONS 2 THROUGH 9 (REFERENCE (P)) SHALL BE CONSIDERED AS BEING FOUO. FOUO IS NOT AUTHORIZED AS A WEAK FORM OF CLASSIFICATION TO PROTECT U.S. NATIONAL SECURITY INTERESTS .

1-339 VIDEO TAPE (TWO WORDS)

A MAGNETIC TAPE USED FOR THE ELECTRONIC RECORDING AND PLAYBACK OF MATERIAL FOR TELEVISION APPLICATION.

1-340 VIDEOTAPE (ONE WORD)

VIDEO TAPE ON AN OPEN REEL.

1-341 VIDEOCASSETTE

VIDEO TAPE ON REELS IN A SEALED CONTAINER THAT IS USED IN A RECORD OR PLAYBACK MODE WITHOUT REMOVAL FROM THAT CONTAINER .

1-342 VIOLATION

A SECURITY VIOLATION IS CONSTITUTED BY ANY FAILURE TO SAFEGUARD CLASSIFIED INFORMATION OR ANY FAILURE, WITTING OR UNWITTING, TO COMPLY WITH THIS INSTRUCTION .

Section 4

POLICIES

1-400 Classification

a. Basic Policy. Except as provided in the Atomic Energy Act of 1954, as amended (reference (l)), E.O. 12356 (reference (g)), as implemented by the 1S00 Directive No. 1 (reference (h)), and this Regulation, provides the only basis for classifying information. It is the policy of the Department of Defense to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

b. Resolution of Doubts. Umecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it 'were classified "Confidental" pending a determination by an original classification authority, who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within 30 days. Upon a classification determination, markings shall be applied in accordance with Chapter IV.

c. Duration. Information shall be classified as long as required by national security considerations. Each decision to classify requires a simultaneous determination of the duration such classification must remain in force or that the duration of classification cannot be determined.

1-401 Declassification

Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or upon the occurrence of a declassification event.

1-402 Safeguarding

Information classified under this Regulation shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions that may arise in connection with its use, dissemination, storage, movement or transmission, and destruction.

Section 5

SECURITY CLASSIFICATION DESIGNATIONS

1-500 General

Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one

of three designations, namely: "Top Secret," "Secret," or "Confidential." The markings "For Official Use Only," and "Limited Official Use" shall not be used to identify classified information. Moreover, no other term such as "Sensitive, " "Conference," or "Agency" shall be used in conjunction with the authorized classification designations to identify classified information.

SEE CHAPTER XV, BELOW, FOR POLICY ON THE USE OF THE MARKING "FOR OFFICIAL USE ONLY."

1-501 Top Secret

"Top Secret" shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

1-502 Secret

"Secret" shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

1-503 Confidential

"Confidential" shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, ❑aintenance, and inspection of classified ❑unitions of war; revelation of performance characteristics, test data, design, and production data on munitions of war.

Section 6

AUTHORITY TO CLASSIFY, DOWNGRADE, AND DECLASSIFY

1-600 Original Classification Authority

a. Control. Authority for original classification of information as Top Secret, Secret, or Confidential may be exercised only by the Secretary of Defense, the Secretaries of the Military Departments, and by officials to whom such authority is specifically delegated in accordance with and subject to the

restrictions of this Section of the Regulation. In the absence of an original classification authority, the person designated to act in his or her absence may exercise the classifier's authority.

b. Delegation of Classification Authority. Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source ❑aterial or as directed by a classification guide. Delegations of original classification authority shall be limited to the minimum number required for efficient administration and to those officials whose duties involve the origination and evaluation of information warranting classification at the level stated in the delegation.

1. Top Secret. Only the Secretary of Defense, the Secretaries of the Military Departments, and the senior official designated by each under Section 5.3(a) of E.O. 12356 (reference (g)), provided that official has original Top Secret classification authority, may delegate original Top Secret classification authority. Such delegation may only be made to officials who are determined to have a demonstrable-and continuing-need to -exercise such authority.

2. Secret and Confidential. Only the Secretary of Defense, the Secretaries of the Military Departments, the senior official designated by each under Section 5.3(a) of reference (g), and officials with original Top Secret classification authority, may delegate original Secret and Confidential classification authority to officials whom they determine respectively to have a demonstrable and continuing need to exercise such authority.

3. Each delegation of original classification authority shall be in writing and shall specify the title of the position held by the recipient.

c. Requests for Classification Authority

1. A request for the delegation of original classification authority shall be made only when there is a demonstrable and continuing need to exercise such authority and the following conditions exist:

(a) The normal course of operations or missions of the organization results in the origination of information warranting classification;

(b) There is a substantial degree of local autonomy in operations or missions as distinguished from dependence upon a higher level of command or supervision for relatively detailed guidance;

(c) There is adequate knowledge by the originating level to make sound classification determinations as distinguished from having to seek such knowledge from a higher level of command or supervision; and

(d) There is a valid reason why already designated classification authorities in the originator's chain of command or supervision have not issued or cannot issue classification guidance to meet the originator's normal needs.

2. Each request for a delegation of original classification authority shall:

(a) Identify the title of the position held by the nominee and the nominee's organization;

(b) Contain a description of the circumstances, consistent with 1., above, that justify the delegation of such authority; and

(c) Be submitted through established channels to the Secretary of Defense, the Secretary of the Military Department concerned, the senior official designated by each under Section 5.3(a) of E.O. 12356 (reference (g)), or the appropriate Top Secret classification authority. (See subsection 1-602.)

d. Training Requirements for Original Classification Authorities. Heads of DoD Component shall establish procedures to ensure that all original classification authorities in their Component, to include themselves, are indoctrinated in the fundamentals of security classification, limitations on their authority to classify information, and their responsibilities as such. This indoctrination shall be a prerequisite to the exercise of such authority and shall be a matter of record that is subject to audit. Heads of DoD Components shall ensure this indoctrination is given to all present original classification authorities within 12 months of the effective date of this Regulation. A VIDEO TAPE, PREPARED BY THE DEPUTY UNDER SECRETARY OF DEFENSE (POLICY) (DUSD(P)), SHALL BE REVIEWED BY EACH ORIGINAL CLASSIFICATION AUTHORITY.

1-601 Derivative Classification Responsibility

Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information that is already classified, or those who apply markings in accordance with guidance from an original classification authority. Persons who apply derivative classifications should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all *or* part of the basis for classification. Persons who apply such derivative classification markings shall:

a. Respect original classification decisions;

b. Verify the information's current level of classification as far as practicable before applying the markings; and

c. Carry forward to any newly created documents the assigned dates or events for declassification and any additional authorized markings.

1-602 Record and Report Requirements

a. Records of designations of original classification authority shall be maintained as follows:

1. Top Secret Authorities. A current listing by title and organization of officials designated to exercise original Top Secret classification authority shall be maintained by:

(a) The Office of the Deputy Under Secretary of Defense (Policy) (ODUSD(P)) for the Office of the Secretary of Defense; the Organization of the Joint Chiefs of Staff; the headquarters of each Unified Command and the headquarters of subordinate Joint Commands; and the Defense Agencies.

(b) The Offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective departments who are serving in headquarters elements of Unified Commands and headquarters of Joint Commands subordinate thereto.

2. Secret and Confidential Authorities. A current listing by title and organization of officials designated to exercise original Secret and Confidential classification authority shall be maintained by:

(a) The ODUSD(P) for the Office'of the Secretary of Defense.

(b) The offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective departments who are serving in headquarters elements of Unified Commands and headquarters elements of Joint Commands subordinate thereto.

(c) The Director, Joint Staff, for the OJCS.

(d) The Commanders-in-Chief of the Unified Commands, for their respective headquarters and the headquarters of subordinate Joint Commands.

(e) The Directors of the Defense Agencies, for their respective agencies.

3. If the listing of titles of positions and organizations prescribed in subparagraphs 1. and 2., above, discloses intelligence or other information that either qualifies for security classification protection *or* otherwise qualifies to be withheld from public release under statute, some other means may be recommended by the DoD Component by which original classification authorities can be readily identified. Such recommendations shall be submitted to ODUSD(P) for approval.

4. The listings prescribed in subparagraphs 1. and 2., above, shall be reviewed at least annually by the senior official designated in or pursuant to paragraph 13-200a, or subsections 13-301 or 13-302 or designee to ensure that officals so listed have demonstrated a continuing need to exercise original classification authority.

b. The DoD Components that maintain listings of designated original classification authorities shall, upon request, submit copies of such listings to ODUSD(P).

1-603 Declassification and Downgrading Authority

a. Authority to declassify and downgrade information classified under provisions of this Regulation shall be exercised as follows:

1. By the Secretary of Defense and the Secretaries of the Military Departments, with respect to all information over which their respective Departments exercise final classification jurisdiction;

2. By the official who authorized the original classification, if that official is still serving in the same position, by a successor, or by a supervisory official of either; and

3. By other officials designated for the purpose in accordance with paragraph b., below.

4. WITHIN OSD COMPONENTS, DECLASSIFICATION AND DOWNGRADING AUTHORITY SHALL BE EXERCISED BY THE FOLLOWING:

(a) OFFICIAL IDENTIFIED ON THE "CLASSIFIED BY" LINE OF A DOCUMENT OR OFFICIAL'S SUCCESSOR.

(b) OSD ORIGINAL CLASSIFICATION AUTHORITY FOR THE OSD COMPONENT THAT HAS ASSUMED FUNCTIONAL INTEREST, WHEN SUCH INTEREST FOR THE INFORMATION HAS CHANGED.

(c) OSD PRINCIPAL STAFF ASSISTANTS MAY DESIGNATE, BY TITLE OF POSITION, SUBORDINATE OFFICIALS TO EXERCISE GENERAL DECLASSIFICATION AND DOWNGRADING AUTHORITY. A COPY OF ANY SUCH DESIGNATION SHALL BE SUBMITTED TO THE ODUSD(P).

(d) THE ASSISTANT SECRETARY OF DEFENSE (PUBLIC AFFAIRS) ASD(PA) HAS DECLASSIFICATION AUTHORITY SPECIFICALLY DELEGATED IN DOD DIRECTIVE 5122.5, (REFERENCE (ooo)).

5. IN CASES OF DOCUMENTS CONTAINING INFORMATION CLASSIFIED BY OR UNDER THE FUNCTIONAL RESPONSIBILITY OF MORE THAN ONE OSD COMPONENT, DECLASSIFICATION AND DOWNGRADING AUTHORITY CONTINUES TO RESIDE IN THE OFFICIALS DESIGNATED IN PARAGRAPH l-603a. 4., ABOVE. DECLASSIFICATION OR DOWNGRADING SHALL NOT BE TAKEN WITHOUT PRIOR COORDINATION WITH OTHER OSD COMPONENTS.

6. DOCUMENTS ORIGINATED AND CLASSIFIED BY OTHER THEN OSD COMPONENTS SHALL NOT BE DECLASSIFIED BY AN OSD COMPONENT WITHOUT PRIOR WRITTEN PERMISSION OF THE ORIGINATING OFFICE OR AGENCY.

b. The Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Directors of the Defense Agencies or their senior officials designated under subsection 13-301 or 13-302 may designate additional officials at the lowest practicable echelons of command and supervision to exercise declassification and downgrading authority over classified information in their functional areas of interest. Records of officials so designated shall be maintained in the same reamer as prescribed in paragraph 1-602 a. 1. for records of designations of original classification authority.